UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/982,624	10/18/2001	Taizo Shirai	09812.0537-00000	8604

22852 7590 08/02/2006

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
PARTHASARATHY, PRAMILA	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 08/02/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/982,624	SHIRAI ET AL.	
	Examiner	Art Unit	
	Pramila Parthasarathy	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 May 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4 and 6-9* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4 and 6-9* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to remarks filed on 18, May 2006. Presently pending claims are 1 – 4 and 6 – 9.

Double Patenting

2. Applicant's arguments, see Pages 2-3, filed May 18, 2006, with respect to Double Patenting have been fully considered and are persuasive. The Double Patenting rejection of Claims 1 – 4 and 6 – 9 has been withdrawn.

Response to Arguments

3. Applicant's arguments filed May 18, 2006 have been fully considered but they are not persuasive.

Bellare et al. (U.S. Patent Number 5,673,319) teaches a method for encrypting a plaintext string into ciphertext by cipher block chaining (CBC) the plaintext using a first key and an initialization vector to generate CBC message authentication code (MAC).

Regarding claims 1 and 6 –9, Applicant argues that Bellare does not teach, "using a storage key stored in said data storage device" and "using a storage key stored in said data storage device". These arguments are not found persuasive. Bellare discloses that the storage device can be a hard disk or a removable memory. Furthermore, Bellare discloses that the first (secret) key (stored in any of the above said storage devices) and an initialization vector are used to generate a CBC message authentication code (MAC) (Column 5 lines 5 – 21).

Therefore, the examiner respectfully asserts that the cited prior art does teach or suggest the amended subject matter "using a storage key stored in said data storage device" and "using a storage key stored in said data storage device", broadly recited in the independent claims 1 and 6 – 9. The dependent claims 2 – 4 are rejected at least by virtue of their dependency on the dependent claims and by other reason set forth in this office action.

Accordingly, the rejection for the pending claims 1 – 4 and 6 – 9 is respectfully maintained.

Claim Rejections - 35 USC § 102

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

4. Claims 1 – 4 and 6 – 9 are rejected under 35 U.S.C. 102(b) as being clearly anticipated by Bellare et al. (U.S. Patent Number 5,673,319).

Regarding Claim 1, Bellare teaches and describes a data storage area consisting of a plurality of blocks, each of which consists of a plurality of sectors which each have a predetermined data capacity (Summary and Column 5 lines 5 – 21); and

cryptosystem means (Summary and Column 5 lines 5 – 21);

wherein said cryptosystem means receives, as cryptosystem keys for performing cryptosystem processing on data to be stored in said data storage area a first set of keys correlated with the encryption keys or decryption keys for each of the sectors from a device capable of performing data communication with said data storage device and a second set of keys correlated with integrity-check-value generating keys of data to be stored in at least one of the sectors; and transmits the encrypted key to said data storage device (Summary; Column 4 lines 13 – 65 and Column 5 line 5 – Column 6 line 35).

Regarding Claim 6, Bellare teaches and describes executing mutual authentication processing between said data storage device and said data recording device (Summary and Column 5 lines 5 – 21);

when the mutual authentication is established, transmitting, to said data storage device, by said data recording device, a set of session-key-used CBC-mode-processing keys which are generated by executing, based on a session key generated in the

mutual authentication, encryption processing in the CBC mode on a first set of keys applicable to encryption processing on pieces of data to be stored in the sectors and a second set of keys correlating to integrity-check-value generating keys of data to be stored in at least one of the sectors, the encryption processing being executed on said first and second set of keys in the CBC using a storage key stored in said data storage device (Summary; Column 4 lines 13 – 65 and Column 5 lines 5 – 21);

decrypting, by said data storage device, said set of session-key-used CBC-mode-processing keys by performing decryption in the CBC mode using the session key (Summary and Column 5 lines 22 – 34);

transmitting, to said data storage device, a set of decrypting, by storage-key-used generated by executing based on a storage key unique to said data storage device, encryption processing in the CBC mode on the set of decrypted session-key-used CBC-mode-processing keys (Summary and Column 5 line 5 – Column 6 line 35); and

generating, by said data recording device, header information including as a component the received set of storage-key-used CBC-mode-processing keys which are generating, by said data recording device, header information including as a component the received set of storage-key-used CBC-mode-processing keys, the header information corresponding to the data to be stored in said data storage device (Summary; Column 4 lines 13 – 65 and Column 5 line 5 – Column 6 line 35).

Regarding Claim 7, Bellare teaches and describes executing mutual authentication processing between said data storage device and said data playback device (Summary and Column 5 lines 5 – 21);

when the mutual authentication is established, transmitting. from said data playback device to said data storage device, a set of storage-key-used CBC-mode-processing keys which is included in the header information of data stored in said data storage area and which is generated by executing encryption processing in the CBC mode using a storage key unique to said data storage device and on an integrity-check-value generating key of data to be stored in at least one of the sectors (Summary; Column 4 lines 13 – 65 and Column 5 lines 5 – 21);

decrypting, by said data storage device, the set of storage-key-used CBC-mode-processing keys by performing decryption in the CBC mode using the storage key (Summary and Column 5 lines 5 – 34);

transmitting, by said data storage device, to said data playback device, a set of session-key-used CBC-mode-processing keys which are generated by executing, based on a session key generated in the mutual authentication encryption processing in the CBC mode on the set of decrypted storage-key-used CBC-mode-processing keys (Summary and Column 5 line 5 – Column 6 line 35); and

obtaining, by said data playback device, a set of keys for decrypting encrypted sector data which is stored in each of the sectors in said data storage area by decrypting, in the CBC mode, the session-key-used CBC-mode-processing keys by using the session key (Summary and Column 5 line 5 – Column 6 line 35).

Regarding Claim 8, Bellare teaches and describes executing mutual authentication processing between said data storage device and said data recording device (Summary and Column 5 lines 5 – 21);

when the mutual authentication is established, transmitting, to said data storage device, by said data recording device, a set of session-key-used CBC-mode-processing keys which are generated by executing, based on a session key generated in the mutual authentication, encryption processing in the CBC mode on a first set of keys applicable to encryption processing on pieces of data to be stored in the sectors and a second set of keys correlated with integrity-check-value generating keys of data to be stored in at least one of the sectors, the encryption processing being executed using a storage key stored in said data storage device (Summary; Column 4 lines 13 – 65 and Column 5 lines 5 – 21);

decrypting, by said data storage device, said set of session-key-used CBC-mode-processing keys by performing decryption in the CBC mode using the session key (Summary and Column 5 lines 22 – 34);

transmitting to said data storage device, a set of storage-key-used CBC-mode-processing keys which are generated by executing, based on a storage key unique to said data storage device, encryption processing in the CBC mode on the set of decrypted session-key-used CBC-mode-processing keys (Summary and Column 5 line 5 – Column 6 line 35); and

generating, by said data recording device, header information including as a component the received set of storage-key-used CBC-mode-processing keys which are

generating, by said data recording device, header information including as a component the received set of storage-key-used CBC-mode-processing keys, the header information corresponding to the data to be stored in said data storage device (Summary; Column 4 lines 13 – 65 and Column 5 line 5 – Column 6 line 35).

Regarding Claim 9, Bellare teaches and describes executing mutual authentication processing between said data storage device and said data playback device (Summary and Column 5 lines 5 – 21);

when the mutual authentication is established, transmitting, from said data playback device to said data storage device, a set of storage-key-used CBC-mode-processing keys which is included in the header information of data stored in said generated by executing data storage area and which is encryption processing in the CBC mode using a storage key unique to said data storage in at least one of the sectors (Summary; Column 4 lines 13 – 65 and Column 5 lines 5 – 21);

decrypting, by said data storage device, the set of storage-key-used CBC-mode-processing keys by performing decryption in the CBC mode using the storage key (Summary and Column 5 lines 22 – 34);

transmitting, by said data storage device, to said data playback device, a set of session-key-used CBC-mode-processing keys which are generated by executing, based on a session key generated in the mutual authentication, encryption processing in the CBC mode on the set of decrypted storage-key-used CBC-mode-processing keys (Summary and Column 5 line 5 – Column 6 line 35); and

obtaining, by said data playback device, a set of keys for decrypting encrypted sector data which is stored in each of the sectors in said data storage area by decrypting, in the CBC mode, the session-key-used CBC-mode-processing keys by using the session key (Summary and Column 5 line 5 – Column 6 line 35).

Claim 2 is rejected applied as above in rejecting Claim 1. Furthermore, Bellare teaches and describes wherein said cryptosystem means, generates key data as the header information of the data to be stored in said data storage area by using a storage key which is unique to said data storage device to execute the encryption processing in the CBC mode on the received set of keys (Summary and Column 5 line 5 – Column 6 line 35).

Claim 3 is rejected applied as above in rejecting Claim 1. Furthermore, Bellare teaches and describes said data storage with said device capable of performing data communication with said data storage device (Summary and Column 5 lines 5 – 21);

the received set of keys is a set device performs mutual authentication of session-key-used CBC-mode-processing keys a session key generated in the mutual authentication (Summary and Column 5 lines 5 – 21);

said cryptosystem means performs the decryption in the CBC mode of said set of encrypted session-key-used CBC-mode-encrypted in the CBC mode by using processing keys (Summary and Column 5 lines 22 – 34); and

in said cryptosystem means CBC-mode-processing keys is generated by executing, based on a storage key unique to said data storage device, the encryption processing in the CBC mode on the set of decrypted session-key-used CBC-mode-processing keys, and said set of storage-key-used CBC-mode-processing keys is a set of storage-key-used transmitted as header-information-forming data to said device (Summary and Column 5 line 5 – Column 6 line 35).

Claim 4 is rejected applied as above in rejecting Claim 1. Furthermore, Bellare teaches and describes said data storage device performs mutual authentication with said device capable of performing data communication with said data storage device;

the received set of keys is header information on the data to be stored in said data storage area, and is a set of storage-key-used CBC-mode-processing keys encrypted in the CBC mode based on a storage key unique to said data storage device (Summary and Column 5 lines 5 – 21);

said cryptosystem means performs the decryption in the CBC mode of the set of encrypted storage-key-used CBC-mode-processing keys by using said storage key (Summary and Column 5 lines 22 – 34); and

in said cryptosystem means, a set of session-key-used CBC-mode-processing keys is generated by executing, based on a session key generated in the mutual authentication, the encryption processing in the CBC mode, and said set of session-key-used CBC-mode-processing keys is transmitted as data constituting decrypting key information (Summary and Column 5 line 5 – Column 6 line 35).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Examiner's Note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

Applicant is urged to consider the references. However, the references should be evaluated by what they suggest to one versed in the art, rather than by their specific disclosure. If applicants are aware of any better prior art than those are cited, they are required to bring the prior art to the attention of the examiner.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m.. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy
July 24, 2006.

NASSER MOAZZAMI
PRIMARY EXAMINER
7/28/06